UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/899,359	07/05/2001	Joerg U. Ferchau	M-9912 US	2147

7590 09/23/2004

Mr. Joerg Ferchau
iS3 Inc.
19925 Stevens Creek Blvd.
Cupertino, CA 95014

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	**PAPER NUMBER**
2133	

DATE MAILED: 09/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/899,359	FERCHAU ET AL.
	Examiner	Art Unit
	Shewaye Gelagay	2133

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/10/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Requirement for Information

Applicant and the assignee of this application are required under 37 CFR 1.105 to provide the following information that the examiner has determined is reasonably necessary to the examination of this application.

The examiner did not consider the NPL cited on the IDS because the examiner is unable to access the web page as cited in the IDS (the web page dated 8/24/01 is no longer available). In order the cited NPL to be considered, the applicant is advised to submit the full disclosure of the NPL (article).

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 2, 4, 5, 7-10, 12-18, 23, 24, 26, 27, 30-33, 35 and 38-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Clark United States Letters Patent No. 5,448,045.

3. As per claim 1:

Clark teaches a method for validating the integrity of a target data file loaded on a computing device, the method comprising:

providing a portable cryptographic device (corresponding to smartcard 22, Fig 1;) having a software verification key (file signature cryptographic key 46, Fig. 6), the portable cryptographic device being coupled to a computing device (smartcard 22 communicating to a computer device 10, Fig. 1)(through a communication link Col. 5, lines 53-55);

identifying a target data file for validation on the computing device (identifying target data file is understood according to the specification as inputting a target data file at line 27, page 3) (uploading boot information; Col. 10, line 63); and

generating a software verification value for the target data file using the software verification key (host computes file-checksum which the smartcard encrypts to form a signature; Col. 10 lines 65-69).

4. As per claim 2:

Clark teaches storing the software verification value on the portable cryptographic device. (file integrity information; 44 of Fig. 6)

5. As per claim 4:

Clark teaches receiving a user identification; and validating the user identification against a secret user information, wherein the secret user information is provided on the portable cryptographic device (the authorization information may be a password entered by a user and verified by the device with a pre-stored password stored on the smartcard; Col. 5, lines 36-37).

6. As per claim 5:

Clark teaches the user identification comprises a password (the authorization information may be a password; Col. 5, line 37).

7. As per claim 7:

Clark teaches the user identification comprises a biometric data (biometric information such as fingerprint; Col. 5, line 38).

8. As to claim 8:

Clark teaches requesting a previously generated software verification value; and comparing the software verification value with the previously generated software verification value (host computes file-checksum which the smartcard encrypts to form a signature; this value is compared with the signature stored on the card; Col. 10, lines 66-69 to Col. 11, Lines 5-7).

9. As per claim 9:

Clark teaches the software verification value is performed in response to a startup of the target data file (during the system startup or booting; Col. 10, lines 66-69).

10. As to claim 10:

Clark teaches the portable cryptographic device is a smart card. (Col. 5, line 40; e.g. a smartcard; Fig. 1).

11. As to claim 12:

Clark teaches generating the software verification value comprises a secure hashing calculation (Col 13, line 6; for each file compute a hash).

12. As to claim 13:

Clark teaches generating the software verification value comprises an encryption calculation. (Col 13, lines 6-7; for each file compute a hash which is encrypted by the card)

13. As to claim 14:

Clark teaches generating the software verification value comprises a message authentication calculation. (Col 13, lines 11-12; load host authentication information)

14. As to claim 15:

Clark teaches generating the software verification value comprises a digital signature. (Col 13, lines 8-9; the signature together with the file name is stored on the card)

15. As to claim 16:

Clark teaches the target data file comprises an operating system. (Col. 5, lines 42; comprises executable code) (Col. 5, line 43; comprises system data or user data)

16. As to claim 17:

Clark teaches the target data file comprises an application program. (Col. 5, line 42; comprises executable code.) (Col. 5, line 43; comprises system data or user data)

17. As to claim 18:

Clark teaches the software verification value is generated in response to detecting an install of the data file. (Col. 10, lines 19-24; installation and configuration)

18. As to claim 23:

Clark teaches generating the software verification value is performed by executing logic on the computing device. (Col. 10 lines 66-69; host computes file-checksum which the smartcard encrypts to form a signature)

19. Claims 24 and 27 are an apparatus version of claim 1. Therefore, it is rejected on the same basis as claim 1.

20. Claim 26 is an apparatus version of claim 23. Therefore, it is rejected on the same basis as claim 23.

21. Claim 30 is an apparatus version of claim 4. Therefore, it is rejected on the same basis as claim 4.

22. Claim 31 is an apparatus version of claim 8. Therefore, it is rejected on the same basis as claim 8.

23. Claim 32 is a computer-medium readable storage version of claim 1. Therefore, it is rejected on the same basis as claim 1.

24. Claim 33 is a computer-medium readable storage version of claim 23. Therefore, it is rejected on the same basis as claim 23.

25. Claim 35 is a computer-medium readable storage version of claim 18. Therefore, it is rejected on the same basis as claim 18.

26. Claim 38 is a computer-medium readable storage version of claim 4. Therefore, it is rejected on the same basis as claim 4.

27. Claim 39 is a computer-medium readable storage version of claim 8. Therefore, it is rejected on the same basis as claim 8.

28. Claim 40 is a computer-medium readable storage version of claim 9. Therefore, it is rejected on the same basis as claim 9.

Claim Rejections - 35 USC § 103

29. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

30. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

31. Claims 11, 21, 22, 25 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Clark United States Letters Patent No. 5,448,045.

As per claim 11:

Clark substantially teaches the claimed method of a portable cryptographic device to be a pocket-sized card containing the microprocessor and the memory (Col. 5, line 40; e.g. a smartcard; Fig. 1). Not explicitly disclosed by Clark is that "said portable cryptographic device is a USB connected module." However, at the time the invention was made USB port was present in all computers and has been a general connecting device for cameras, cell phones, video players, etc. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Clark to include a portable cryptographic device that is a USB connected module. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so in order to facilitate the portable cryptographic device to be coupled or connected with appliances like cameras, cell phones, TV or video players.

As per claim 21 and 22:

Clark teaches a method as disclosed above of generating the software verification value is performed by logic executing on the computing device. Clark further teaches all cryptographic operations can be performed in their entirety on the card (Col. 8, lines 37-38), which would imply that logic or logic executing on the smartcard can be performed to generate the software verification value. Clark does not explicitly disclose a logic or logic executing on the portable cryptographic device to generate a software

verification value. However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Clark's method to include logic or logic executing on the portable cryptographic device to generate software verification value. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to have the card provide strong security. This way, all secret information is utilized solely within the confines of the card. (Col. 8, lines 33-35).

As per claim 25:

Claim 25 is an apparatus version of claim 22. Therefore, it is rejected on the same basis as claim 22.

As per claim 34:

Claim 34 is a computer-medium readable storage version of claim 22. Therefore, it is rejected on the same basis as claim 22.

32. Claims 3, 28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Clark United States Letters Patent No. 5,448,045 and in view of Hannah et al. United States Letters Patent No. 6,735,696.

As per claim 3:

Clark teaches the claimed method for storing the software verification value on a portable cryptographic device. Clark does not explicitly teach storing the software verification value on the computing device as required by claim 3.

Hannah et al. in an analogues art, however, teach a software verification value (which is called hash value Col. 2, line 32) is provided on a flash unit memory in the computer which determines whether the software code is executed or not.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify the method disclosed by Clark to include a method comprising storing the software verification value on the computing device. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the suggestion provided by Hannah et al., to have an option of implementing Clark's method with or without a portable cryptographic device.

As per claims 28 and 29:

Claims 28 and 29 are an apparatus version of claim 3. Therefore, they are rejected on the same basis as claim 3.

33. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Clark United States Letters Patent No. 5,448,045 and in view of Schaeck et al. United States Patent Letters No. 6,775,398.

34. As per claim 6:

Clark teaches the claimed method for authorization information to include a password entered by a user and verified by the device or biometric information. Clark does not explicitly disclose including a personal identification number (PIN) as part of the authentication process.

Schaeck et al. in analogous art, however, teach the authentication value, for example PIN, is entered and compared with the reference PIN (Col. 2, lines 7-9). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Clark to include a personal identification number as part of the authentication process. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the suggestions, provided by Schaeck et al., to include personal identification number in addition to the password and biometric data disclosed by Clark, in order to further enforce the smartcard use functions under the exclusive control of the authorized user.

35. Claims 19, 20, 36 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Clark United States Letters Patent No. 5,448,045 and in view of Flint et al. United States Patent Letters No. 6,735,700.

As per claim 19:

Clark teaches the claimed method for generating software verification value in response to detecting an install of the data file. Clark does not explicitly disclose generating software verification value in response to detecting a closing of the data file.

Flint et al. in an analogous art, however, teach anti-virus software that creates session key for each execution of the software (see Abstract). Flint et al. further teach scanning can be done upon request of a user, when the file is accessed on a mass storage device such as by an application or on scheduled basis (Col. 1, lines 41-43).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Clark to include a method comprising generating software verification value in response to detecting a closing of the data file. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the suggestions, provided by Flint et al., to generate software verification value in response to detecting a closing of the data file, in order to verify the integrity of the data file when the file is accessed again.

As per claim 20:

Clark teaches the claimed method for generating software verification value in response to detecting an install of the data file. Clark does not explicitly disclose generating software verification value in response to detecting a shutdown of the computing device.

Flint et al. in an analogous art, however, teach anti-virus software that creates session key for each execution of the software (see Abstract). Flint et al. further teach scanning can be done upon request of a user, when the file is accessed on a mass storage device such as by an application or on scheduled basis (Col. 1, lines 41-43).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Clark to include a method comprising generating software verification value in response to detecting a shutdown of the computing device. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by suggestions,

provided by Flint et al. in order to verify the integrity of the data file when the file is accessed again.

As per claim 36:

Claim 36 is an apparatus version of claim 19. Therefore, it is rejected on the same basis as claim 19.

As per claim 37:

Claim 37 is an apparatus version of claim 20. Therefore, it is rejected on the same basis as claim 20.

36. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 703-305-1338. The examiner can normally be reached Monday to Friday from 8:30 am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 703-305-9595. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay
Patent Examiner
Art Unit 2133